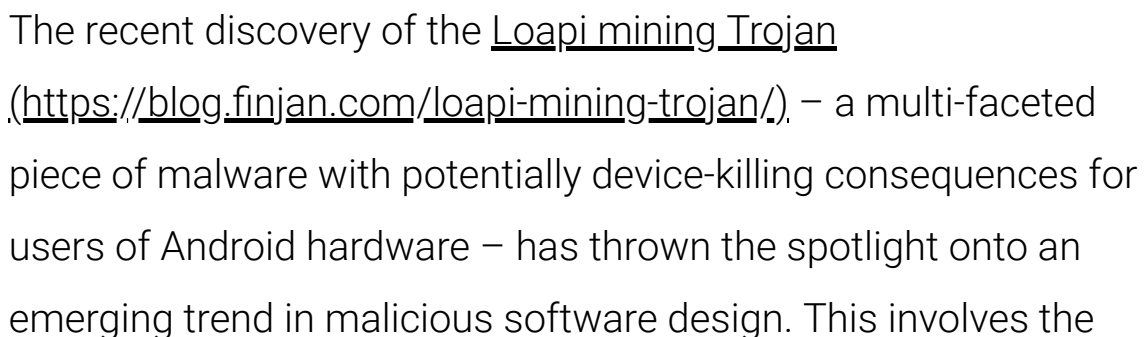


**CYBERRISK**  
**(<https://www.cyberrisk.biz/>)**



Cybersecurity (<https://www.cyberisk.biz/category/cybersecurity/>).



engineering of malware code aimed at co-opting the system resources of a victim's hardware, for the purpose of mining cryptocurrencies.

This process has been dubbed “**cryptojacking**”, and its methodology and implications for cyber-security will form the basis of discussion for this article.

## **Cryptojacking – Incentives for Bad Behavior**

Frenetic activity continues in the cryptocurrency. (<https://www.cyberisk.biz/blockchain-and-virtual-currency/>), sector, with recent dramatic hikes and plunges in the value of Bitcoin and other denominations hitting the mainstream news. With such wild fluctuations and the relative immaturity of the market, there's plenty of money to be made – and not only by the investors.

Cryptocurrencies are generated through the digital process of mining (<https://www.scientificamerican.com/article/is-your-computer-secretly-mining-bitcoin-alternatives-a-guide-to-ldquo-cryptojacking-rdquo/>), whereby users participating in a mining scheme dedicate a proportion of their system's processing and computing power to the solution of complex mathematical problems, in anticipation of the award of cryptocurrency credits for a successful calculation.

Many cryptocurrency miners across the globe submit to this process willingly, as a potential revenue stream for themselves. But cyber-criminals have also warmed to the idea, and to the notion of

tricking unsuspecting computer owners into contributing their system resources to the mining effort unwittingly.

It's been estimated that 220 of the top 1,000 websites in the world are conducting cryptojacking operations, making a total of \$43,000 over a three week period. Though some of them are doing it with the consent of their site visitors, the majority of cryptojackers are working under the veil of secrecy.

It's a cheaper and lower-risk strategy than ransomware distribution – and offers the potential for far greater financial rewards, over a sustained period. And there's an entire ecosystem emerging to assist these perpetrators in their cryptojacking efforts.

## **Facilitating Measures**

Mining activity for Bitcoin (the most high-profile of the cryptocurrencies) is a complex process requiring specialized hardware and a huge amount of energy. It's been estimated that each Bitcoin mining transaction consumes enough energy to boil around 36,000 kettles filled with water – and that in a single year, the global Bitcoin mining operation consumes more energy than the Republic of Ireland.

Lacking such huge resources, “citizen” cryptocurrency miners, therefore, turn to less intensive alternatives, such as Monero, which requires no specialized computing equipment.

In mid-September 2017, a company named Coinhive launched a piece of commercial software that can be written into the content of a web page (typically in the form of an ad), using the common language of JavaScript. When such a page loads, the script starts mining the Monero cryptocurrency, in the background.

Torrenting website The Pirate Bay almost immediately snapped it up (<https://www.wired.com/story/cryptojacking-cryptocurrency-mining-browser/>), pitching the donation of some processor time to their users as an alternative to in-page advertising. And Coinhive clones of various stripes have been emerging, ever since.

Many developers of these mining programs are touting them as an alternative revenue stream for websites, and some sites have already adopted a “mining with consent” policy in fund-raising for charitable causes such as disaster relief. Coinhive has introduced a new version of its product, known as AuthedMine, which requires authorization/consent (<https://www.wired.com/story/cryptojacking-has-gotten-out-of-control/>), from users before their systems can be co-opted for Monero mining.

But with the vast majority of cryptocurrency mining software offering no opt-in or opt-out choices to the user – and with the programs typically running discreetly beneath the surface – unsuspecting web surfers are still very much victims of the cryptojacking phenomenon.

## No Need to Install

The JavaScript medium used in Coinhive, AuthedMine, and the like ensures that the code required for cryptocurrency mining doesn't have to be installed as a separate application, and can run in any standard web browser. Once a page containing the relevant script is loaded, the program runs automatically – eliminating the need to announce its presence, or ask for user consent.

Hackers have already been successful in introducing cryptojacking scripts onto the Showtime and PolitiFact websites, and on eCommerce platforms. A Starbucks Wi-Fi hotspot in Buenos Aires (<https://slate.com/technology/2018/02/what-is-cryptojacking-the-bitcoin-and-monero-mining-process-that-steals-your-computing-power-explained.html>), Argentina was hijacked in December 2017 by enterprising hackers who tapped into the system resources of fellow coffee-drinkers to boost their mining efforts.

And in January of this year, cryptojacking code was discovered in Archive Poster (<https://www.inverse.com/article/39855-cryptocurrency-google-chrome-mining-monero>), a Chrome browser extension designed to facilitate user interactions with Tumblr posts stored in archives. The extension has since been withdrawn, but given their relative ease of construction, we can expect to see more variants on the Monero-mining code popping up (or rather, hiding in the shadows), in future.

## Device-Killing Overheads

There's been less of an uproar over the cryptojacking trend than for some malware phenomena such as ransomware, as the in-browser code now doing the rounds is often subtle (creating little discernible impact on a victim's system performance), and not actively doing damage to information or files.

However, this isn't to suggest that cryptojacking has zero consequences. Besides the deceit and privacy violation of software that runs without a user's knowledge or consent, there can be discernible effects on enterprise networks affected by the software, and for victims of cryptojacking using mobile devices.

For the enterprise, the stolen CPU cycles of a massive cryptojacking exercise could slow down network operations and have a negative impact on business continuity and overall system availability. Time, money, and effort devoted to IT troubleshooting and help desk activities in tracing the root of the problem and replacing network components or complete systems might also take a serious toll.

Individual computer or mobile device owners will typically notice a slowing down of their systems if affected by a cryptojacking attack. If the assault continues for any length of time, the increased load on their processor may lead to rising device or system temperatures, and thermal stresses on their batteries. In extreme cases (such as with the Loapi mining Trojan), the rise in battery temperature may be sufficiently high to kill off a smartphone or tablet, entirely.

When you bear in mind that many perpetrators rely on a combination of in-browser cryptojacking scripts and targeted malware for their operations, the risk to mobile hardware remains a viable one.

## **Counter-Measures and Protection**

As cryptocurrency mining code is being developed with an eye to thwarting signature-based methods of detection, standard anti-virus and endpoint protection tools are not a reliable defense against cryptojacking.

Far more effective is the creation of a safer browsing environment, through the installation and proper configuration of ad-blocking and anti-cryptomining extensions. Web filtering tools should also be regularly updated to reflect the discovery of websites and pages that deliver cryptojacking scripts.

A mobile device management

(<https://www.csoononline.com/article/3253572/internet/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html>).

(MDM) system can facilitate the enterprise-wide enforcement of whitelisted sites and applications, and remains the best option for organizations which maintain a Bring Your Own Device (BYOD) policy.

As far as security awareness training goes, efforts should focus on educating users to identify and avoid social engineering and phishing strategies which aim at steering victims to sites operating


cryptojacking scripts, or facilitating the infection of user devices with cryptocurrency mining malware.

SHARE THIS POST



(mailto:?  
subject=Cryptojacking%20-%20What%20is%20it%20and%20Opt%20Your%20Devices?  
&body=Hey,%20thought%20yo



Summary	
	
Article Name	Cryptojacking   What is it and How Can it Co-Opt Your Devices?
Description	The discovery of the Loapi Mining Trojan (malware with potentially device-killing consequences for users of Android hardware) has thrown the spotlight onto an emerging trend in malicious software design - malware aimed at co-opting the system resources of a victim's hardware, for the purpose of mining cryptocurrencies.
Author	CybeRisk
Publisher Name	CybeRisk Security Solutions
Publisher Logo	





Tags: [cryptocurrency](https://www.cyberisk.biz/tag/cryptocurrency/),  
[\(https://www.cyberisk.biz/tag/cryptocurrency/\)](https://www.cyberisk.biz/tag/cryptocurrency/),  
[cybersecurity](https://www.cyberisk.biz/tag/cybersecurity/) (<https://www.cyberisk.biz/tag/cybersecurity/>),  
[malware](https://www.cyberisk.biz/tag/malware/) (<https://www.cyberisk.biz/tag/malware/>).

🔍 Search

Schedule a  
FREE Consultation!

First Name

Last Name

Email

Message

☒ Yes, Sign me up for the mailing list

SEND

I'm not a robot

reCAPTCHA

[Privacy](#) - [Terms](#)

or Call 646 517 1146 (tel:+6465171146) Now!



(<https://www.finjanmobile.com/vital->

[security-vpn-4/](#)).

## Recent Posts

[Cryptojacking – What is it and How Can it Co-Opt Your Devices?](#)

(<https://www.cyberisk.biz/cryptojacking/>).

[What is Cyber Resilience and Why Is It Important to My Company?](#)

(<https://www.cyberisk.biz/what-is-cyber-resilience/>).

Top 6 Reasons to Use a VPN (<https://www.cyberisk.biz/reasons-to-use-a-vpn/>).

---

Darknet – Is it all “dark” or is there some light in there?  
(<https://www.cyberisk.biz/darknet-is-it-all-dark-or-is-there-some-light-in-there/>).

---

Top 10 Cyber Security Trends for 2018 (<https://www.cyberisk.biz/top-10-cyber-security-trends-for-2018/>).

---

The Active Cyber Defense Certainty Act – What is it and What are the Pros and Cons? (<https://www.cyberisk.biz/active-cyber-defense-certainty-act/>).

---

General Data Protection Regulation or GDPR  
(<https://www.cyberisk.biz/general-data-protection-regulation-gdpr/>).

---

Gray Hat Hackers and the Gray Areas of Security Vulnerability Reporting  
(<https://www.cyberisk.biz/gray-hat-hackers-security-vulnerability-reporting/>).

---

The Security vs Customer Experience Dilemma – What Comes First in Software Design? (<https://www.cyberisk.biz/security-vs-customer-experience-dilemma/>).

---

Securing Mail Relay is a Priority For Any Enterprise Security Program  
(<https://www.cyberisk.biz/securing-mail-relay/>).

---

Penetration Testing – The Connection Between Pen-Testers and Lockpicking (<https://www.cyberisk.biz/penetration-testing-the-connection-between-pen-testers-and-lockpicking/>).

---

The Chief Information Security Officer – What Role Does the CISO Play Today? (<https://www.cyberisk.biz/the-chief-information-security-officer->

what-role-does-the-ciso-play-today/).

---



(https://www.facebook.com/CyberRisk.com/compare)

Security- trk=tyah&trkInfo=clickedVertical%

Solutions 5490 57891105?

fref=ts)(https://twitter.com/CyberRisk18189351723470216

SOLUTIONS (HTTPS://WWW.CYBERISK.BIZ/SOLUTIONS/).  
/ NEWS (HTTPS://WWW.CYBERISK.BIZ/CATEGORY/NEWS/). / BLOG (HTTPS://WWW.CYBERISK.BIZ/BLOG/).  
/ FINJAN (HTTPS://WWW.FINJAN.COM/). / CONTACT CYBERISK (HTTPS://WWW.CYBERISK.BIZ/CONTACT/).  
/ PRIVACY POLICY (HTTPS://WWW.FINJAN.COM/PRIVACY-POLICY/).